METHOD AND SYSTEM FOR GENERATING A COMMON SECRET KEY

BACKGROUND OF THE INVENTION

The invention relates to a method for generating a common secret data item between a first user facility and a second user facility through by each such user facility executing mutually symmetric operations on respective complementary data that are based on respectively unique quantities that are at least in part secret, and wherein an outcome of said operations is used in both said user facilities as said common secret data item as has been furthermore recited in the preamble of Claim 1.

Shared key generation is an important issue in cryptography. The issue has spread to application fields such as Pay TV Systems in consumer electronics and various identification procedures. The secret data item may be used as an encryption or decryption key, for effecting mutual authentication among the user facilities, or other. Prior art has widely considered Diffie-Hellmann schemes, but these schemes disadvantageously lack a control mechanism for checking the authenticity of the calculated secret data item. Alternatively, a certificate based system allows to set up the shared secret data item has been proposed in US Patent 5,218,637, attorney docket PHQ 90.021 assigned to the present assignee, and among others by one of the coinventors of the present invention. This art solves the problem, but on the other hand requires a complex organization utilizing at least two levels of public key cryptography. A first object of the present invention is to use only a single integrated cryptography level. This implies that no second secret data item will be required to effect a verification operation.

A further object of the present invention is that the system should be extendable with extra user facilities offering the same level of secrecy as the existing system realized by the invention, but without requiring additional amendations to such existing system. Still another object of the present invention is that knowledge of the secret data items pertaining to an arbitrarily large subset of the user facilities should not allow a straightforward and feasible calculation of the respective secret data item for any further user facility present in the system. A further object of the present invention is to allow a compact representation of the various quantities and data items used.

SUMMARY TO THE INVENTION

In consequence, amongst other things, it is an object of the present invention to provide an improved method for generating a common secret data item among two user facilies whilst meeting the above requirements.

Now therefore, according to one of its aspects the invention is characterized according to the characterizing part of Claim 1. In particular, a first embodiment of the present invention bases on the usage of the so-called Weil Pairings that have been amply discussed in the explicit paper presented on CRYPTO 2001 by Dan Boneh & Matt Franklin, entitled "Identity Based Encryption from the Weil Pairing". Furthermore, a second and even broader embodiment of the present invention bases on het usage of the so-called Abelian Varieties, and of which elliptic curves on which the Weil Pairings are effected constitute a sub-class. None of the above concepts have however been considered for the same manner of operating and objects as the present invention. Abelian varieties have been amply discussed in the explicit paper presented on CRYPTO 2002 by K. Rubin & A. Silverberg, entitled "Supersingular Abelian Varieties in Cryptology". A further advantageous aspect of the present invention is that it will allow compact representations due to the straightforward mathematical procedures effectively used.

The invention also relates to a system comprising a first user facility and a second user facility, and being arranged to communicate according to the method as claimed in Claim 1, to a device being arranged to operate as the first and/or second user facility in a system as claimed in Claim 3, and to a computer program product comprising computer instructions for controlling one or more data processing oriented hardware entities to implement a method as claimed in Claim 1. Further advantageous aspects of the invention are recited in dependent Claims.

BRIEF DESCRIPTION OF THE DRAWING

These and further aspects and advantages of the invention will be discussed more in detail hereinafter with reference to the disclosure of preferred embodiments, and in particular with reference to the appended Figures that show:

Figure 1, a system comprising various devices that are interconnected via a network and are arranged to operate in accordance with the invention;

Figure 2, a generalization of the system of Figure 1.

MATHEMATICAL SKETCH OF THE PROCEDURE USED

A basic embodiment of the present invention bases on the ***Weil pairing***, which is a bilinear mapping from elliptic curves to finite fields. It is used to express the Discrete Log problem on finite fields in terms of compact representations on an elliptic curve. This procedure allows to use a shared secret data item and further parameters that can have bit lengths less than 200 bits, whilst still presenting codebreakers with computational complexities that compare with, or are larger than those of prior art systems to render such codebreaking effectively unfeasible. The proposed system is furthermore very robust in that knowledge of the data of a finite number of participants will not give away the system secret which otherwise would have allowed the generation of new shared keys with ***arbitrary*** compliant users.

Furthermore, every user or device has its own unique parameters, which allows to set up a revocation scheme on top of the standard scheme for excluding selected devices when such becomes necessary. As such, the system allows the generating of shared secret data items between any pair of users whilst requiring much less storage capacity than classical systems.

Now, the proposed protocol of the present embodiment bases on an ***extended*** version of the Diffie-Hellmann problem. Note that on an elliptic curve **E**, the Computational Diffie-Hellmann (CDH) problem looks as follows. Given a point $P \in E$ and given aP and bP, there exists no algorithm that computes abP in polynomial time. Now, the present invention applies an ***extended Diffie-Hellmann problem*** or ***EDH*** which regarding the present invention is defined as follows:

$$P, aP, bP, a^2P, b^2P \rightarrow abP$$

Admittedly, in the generic model this will still poses a difficult problem for calculating. Incidentally, the ***Decision Diffie-Hellmann*** or ***DDH*** problem on an elliptic curve is quite a bit more simple. The DDH problem is defined according to: when given three points **aP, bP, cP**, wherein $P \in E$, decide whether or not $cP = (a * b)P$. This relative simplicity follows from an efficiently computable bilinear mapping known as the Weil Pairing, which will be further discussed below; furthermore the referenced publications will offer additional information. In particular, such groups where the DDH is relatively simple but CDH is difficult are said to present a GAP Diffie-Hellmann group. Such groups are found in Abelian varieties, of which the supersingular elliptic curves are a subcategory with dimension 1 thereof. Now, of various feasible such elliptic curves where the computational

Diffie-Hellmann problem is difficult but the DDH is much easier, we use the following exemplary embodiment curves:

$$E^{+}: y^2 = x^3 + 2x + 1 \text{ over } F_3$$

$$E^{-}: y^2 = x^3 + 2x - 1 \text{ over } F_3$$

Now, let $< P >$ be a subgroup of E / F_p of prime order q with a security parameter α. This parameter α must be large enough such that the Computational Diffie-Hellmann problem **CDH** is sufficiently difficult, but at the same time not so large as to render the computing of the Decision Diffie-Hellmann inefficiently difficult. Note that the security parameter of the two exemplary curves supra is $\alpha = 6$ (see Boneh). Furthermore, we assume the availability of a ***distortion map D*** or group isomorphism at our disposal so that the point $D(P) \in E / F_p$ is linearly independent of the point **P**. The distortion map principle has been explicitly discussed in the publication by E. Verheul: "Evidence that XTR is more Secure than Supersingular Elliptic Curve Cryptosystems", EUROCRYPT 2001. This distortion map then constitutes an efficiently computable isomorphism between the groups $< P >$ and $< D(P) >$. Note that the elliptic curves of this example are only two among a large plurality thereof.

Now, with two linearly independent points **P** and $D(P)$ we can use the Weil Pairing to solve certain problems. Now, let $E[q]$ denote the subgroup of $E / F_p \alpha$ that is generated by **P** and $D(P)$.In that case, the Weil Pairing is a map according to $e: E[q] \times E[q] \rightarrow F^{*}_p$, and which satisfies the following properties:

1. For $P \in E[q]$ we have $e(P, P) = 1$.
2. For all $P1, P2 \in E[q]$, and $r, s \in Z$, we have $e(aP1, bP2) = e(P1, P2)^{ab}$, the bilinearity property.
3. If for $P \in E[q]$ one has that $e(P, P') = 1$ for all $P' \in E[q]$, then $P = O$: the non-degeneration property.
4. For all $P1, P2 \in E[q]$, the Weil Pairing $e(P1, P2)$ can be computed efficiently: the computability property.

Then, the following scheme is set up. Each of two user facilities gets the following secret data items from a trusted third party, which items hereinafter being listed for user i (note that the trusted party may be one of the two cooperating user facilities):

5. $(t_{11} + r_i t_{12}) P$
6. $(t_{12} + r_i t_{22}) P$

Furthermore, the following two data items are provided as well:

7. $r_i D(P)$

$8.\ r_1^2 D(P)$

However, the latter two data items need not necessarily be kept secret, and in consequence may for example be stored in a public directory for later consultation. Furthermore, the following symmetric matrix T ($T_{12} = T_{21}$) is defined:

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{12} & t_{22} \end{pmatrix} \in M_2(Z_q)$$

Furthermore, we introduce the vectors $v(r)$ that are associated to a point $r \in Z_q$ as follows: $v(r) = (1, r)$. Now, thereafter the protocol proceeds as follows:

First, User 1 sends data $r_1 D(P), r_1^2 D(P)$ to User 2, and furthermore, User 2 sends data $r_2 D(P), r_2^2 D(P)$ to User 1, followed by user 1 checking whether the triple $r_2 D(P), r_2 D(P), r_2^2 D(P)$ is a Diffie-Hellmann triple, and user 2 checking whether the triple $r_1 D(P), r_1 D(P), r_1^2 D(P)$ is a Diffie-Hellmann triple, and in the positive case both calculate the shared key by user 1 according to $\Pi_{i=1}^2 e((t_{i1} + r_1 t_{i2}) P, v(r_2)_i D(P)) = e(P, D(P))^{\langle v(r_1), Tv(r_2)\rangle}$, the secret common key. Herein $t_{12} = t_{21}$ and $v(r_2)$ stands for the i-th component of the vector $v(r_2)$. It can be proven that the security of the above protocol is high. The security in effect primarily resides on the finding that the ***Extended Diffie-Hellmann*** problem is difficult.

Additional measures to further raise the security level are a hashing of the generated shared key together with the applying of a time stamp. Furthermore, the generating protocol for generating a shared secret can be used as an initial step of an identification procedure as disclosed in EP Patent Application 02 075 983.3, attorney docket PHNL020192 and assigned to the same assignee as the present Application.

Furthermore, the protocol can be made more efficient by already computing the evaluation of the Weil Pairing $e((t_{11} + r_1 t_{12}) P, D(P))$ in advance. This will avoid the necessity to do the computation of this Weil Pairing at the execution of the protocol proper, although at a trading-off price of a raised storage requirement.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Figure 1 illustrates a system 100 comprising various devices 101-105 that are interconnected via a network and are arranged to operate in accordance with the invention.

By way of example, the system is an in-home system, that may comprise devices such as a radio receiver, a television set, etcetera. Generally, a particular device is the system master, and will control the others. Content is generally received through one or more of the devices, such as a residential gateway or settop box 101, from an external source, such as broadband, Internet or satellite. Eventually, the content is transferred over the network for appropriate rendering in one of the devices.

Typically, all devices in the in-home network will implement the security framework in accordance with the implementation requirements. Using this framework, these devices can authenticate each other and distribute content in a secure manner. Access to the content proper will be managed by the security system. This will prevent against unprotected content leaking away to unauthorized devices and also, against data originating from untrusted devices entering into the system. With such protection, devices may only distribute content to other devices which they have succesfully authenticated beforehand. This ensures that an adversary may not receive unauthorized copies through a malicious device. A particular device will only be able to succesfully authenticate itself if it was built by an authorized manufacturer, for example because only authorized manufacturers will know a particular secret that is necessary for succesful authentication, because their devices are provided with a certificate issued by a Trusted Third Party.

Figure 2 illustrates a generalization of the system of Figure 1. Here, a Prover P, a Verifier V, and a trusted third party TTP cooperate. Now, the Verifier V should want to authenticate the prover P through using information received from the Trusted Tird Party TTP. Preferably, the authentication should be mutual, so that also the Prover P would know that the Verifier V were authentic.

The information necessary to authenticate the Verifier V to the Prover P is assumed to have been distributed beforehand from the TTP to the parties P and V. This can be done over a suitable communication facility between the three parties. This renders the protocol dynamic and allows updating of the information in case an adversary would manage to obtain unauthorized access to a secret distributed previously.

The prover P and verifier V can be devices such as carrier 120 in Figure 1, that is equipped with a chip that provides the necessary functionality, and furthermore the audio playback device 105. In such case, there will most likely be no communication channel from the TTP to Prover P and Verifier V. Distribution of the secrets must then be effected beforehand, such as during manufacturing.

Now, the prover comprises a networking module 301, a cryptographic processor 302, and a storage medium 303. Using the networking module 301, Prover P can transmit and receive data with respect to the Verifier V. The networking module 301 could be connected to the network 110 in Figure 1, or rather establish a direct connection such as wireless with the verifier V.

The cryptographic processor 302 is arranged to execute the method according to the present invention. Usually, this processor 302 will be realized as a combination of hardware and software, but alternatively it could be realized entirely in either one of these, such as by a collection of software modules or objects.

Now the Prover P may store in the storage medium various parameters of the algorithm to execute, but it may furthermore also hold some content to distribute to the Verifier V after succesful authentication. The storage medium 303 may furthermore be used to store the information received from the TTP. To enhance the security of the system, rather than storing the individual parameter data, one or more intermediate calculation results could be stored instead or additionally.

Similarly, the Verifier V comprises a networking module 311, a cryptographic processor 312, and a storage facility 313 with the functionality thereof corresponding to that of the Prover P. If the Verifier V is embodied as a carrier with a Chip-in-Disc, then the storage facility 313 may correspond to the storage available to any optical or other disc, but will preferably be stored in ROM of the Chip-in-Disc.

Additionally, the Prover P and the Verifier V may be provided with a pseudo-random number generator 304, 314 that is realized in hardware or software, and provides cryptographically strong pseudo-random numbers. These numbers are used in various preferred applications of the present invention.

SUPPLEMENTARY MATHEMATICAL REPRESENTATION

Hereabove, the generation of the common secret key was effected according to:

$$K_{ij} = F(S_i, P_j) = = F(S_j, P_i)\, K_{ji},$$

Whereas the following data were transferred:

$$S_i = f_T(r_i) \qquad (5, 6), \text{ and}$$

$$P_i = g(r_i) \qquad (7, 8)$$

Another representation of the transmitted data items is according to

S_i	$s_{i1} = T_{11} + r_i T_{12}$	(5')
	$s_{i2} = T_{21} + r_i T_{22}$	(6')
P_i	$p_{i1} = r_i P$	(7')
	$P_{i2} = r_i^2 P$	(8')

Here, $T_{ij} = t_{ij} * P$, and the numerals indicating the correspondence with the earlier representation.